UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/606,089	06/25/2003	Brian S. Christian	MS1-1512US	4285

22971 7590 05/29/2007

MICROSOFT CORPORATION
ONE MICROSOFT WAY
REDMOND, WA 98052-6399

EXAMINER	
WILLIAMS, JEFFERY L	

ART UNIT	PAPER NUMBER
2137	

NOTIFICATION DATE	DELIVERY MODE
05/29/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

roks@microsoft.com
ntovar@microsoft.com
a-rydore@microsoft.com

Office Action Summary	Application No.	Applicant(s)	
	10/606,089	CHRISTIAN ET AL.	
	Examiner	Art Unit	
	Jeffery Williams	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 March 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,4-12,16-21 and 24-28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1, 4-12, 16-21, and 24-28* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This action is in response to the communication filed on 3/22/2007.

All objections and rejections not set forth below have been withdrawn.

Claims 1, 4-12, 16-21, and 24-28 are pending.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1, 4-12, 16-21, and 24-28 are rejected under 35 U.S.C. 102(b) as being anticipated by Scott et al. (Scott), "Abstracting Application-Level Web Security".

Regarding claim 1, Scott discloses:

receiving data input through a web page from a client device (fig. 1, page 2, col. 1, par. 3-6)*; referencing a declarative module to determine a client input security screen to apply to the data input from the client device* (page 3, col. 2, par. 2)*;*

wherein the declarative module comprises:

a global section that includes at least one client input security screen that applies to any type of client input value (fig. 2; page 6, col. 1, par. 1, 2, par. 2, lines 9-13). Scott discloses input security screens (i.e. a transformation screen) that are applied to all user input (parameters values);

an individual values section that includes at least one client input security screen that applies to a particular type of client input value (fig. 2; page 4, col. 1). Herein, Scott discloses screens for screening particular types of client input values (i.e. cookies, urls, other parameters). Thus Scott discloses an individual values section.

and applying multiple client input security screens to the data input from the client device (page 3, col. 2, par. 2; fig. 2), *including at least one client input security screen from the global section of the declarative module and at least one client input security screen from the individual values section of the declarative module, wherein the client input security screens are distinct from one another* (page 3, col. 2, par. 1, 2; fig. 2). Herein, Scott discloses separate screens.

and wherein said act of referencing comprises first using the global section to screen one or more client input values and then using the individual values section to screen at least one of said one or more client input values (sect. 3.4, par. 3).

Regarding claim 4, Scott discloses:

wherein the particular type of client input value is one of the following types of client input values: query string; server variable; form value; cookie (Scott, fig. 2).

Regarding claim 5, Scott discloses:

wherein the declarative module further comprises a web.config file (Scott, page 1, col. 2, par.3; page 3, col. 2, par. 1).

Regarding claim 6, Scott discloses:

wherein the applying the client input security screen further comprises executing a default action on invalid client input detected by the client input security screen (Scott, page 3, col. 2, par. 1, lines 8-13, par. 2, lines 5-11; page 4, col. 2, par. 3,4). Scott discloses the application of several types of input screening to all input data (default screening) wherein actions are performed on the all the input data during the process of data input security screening. Additionally, Scott discloses default transformations that can be applied during the screening of invalid input data.

Regarding claim 7, Scott discloses:

wherein the applying the client input security screen further comprises executing a specified action on invalid client input detected by the client input security screen, the specified action being specified in the client input security screen (Scott, page 4, col. 1, par. 4-6).

Regarding claim 8, Scott discloses:

wherein a client input security screen further comprises one or more values that may be entered as client input, the one or more values further comprising the only

values that may be entered as client input (Scott, page 4, col. 1, par. 4-6). Scott discloses a security screen that constrains client input to a set of values, such as any integer: 0 – int [length 4]. Thus, the security screen effectively comprises the values of 0 – int [length 4] to be imposed upon the client input as a restriction. Additionally, Scott discloses that the security screen comprises specific URL values (extracted from HTTP requests) that may be entered as client input (Scott, page 6, col. 2, par. 1).

Regarding claim 9, Scott discloses:

wherein a client input security screen further comprises one or more screened values that, when detected in the client input, cause an action to be taken on the client input (Scott, fig. 4; page 3, col. 2, par. 2; page 4, col. 2, par. 3).

Regarding claim 10, Scott discloses:

wherein the action to be taken further comprises removing the one or more screened values detected in the client input (Scott, fig. 4; page 3, col. 2, par. 2; page 4, col. 2, par. 3, 4). Scott discloses the encoding of screened values (removal and replacement). Additionally, Scott discloses the removal of values from client input based upon the client input security screen (Scott, page 7, col. 2, par. 1.1 – 1.2)

Regarding claim 11, Scott discloses:

wherein the action to be taken further comprises removing an entire string that contains the one or more screened values detected in the client input (Scott, page 6, col. 2, par. 3; fig. 5; page 9, col. 1, par. 2.2).

Regarding claim 12, it is the system claim corresponding to the method claim 1, and is rejected for, at least, the same reasons, and furthermore because Scott discloses:

a web page server unit configured to provide one or more web pages to one or more client devices over a distributed network (Scott, fig. 1).

Regarding claim 16, Scott discloses:

wherein a screening rule further comprises a client input variable that may be accepted as input from a client (Scott, fig. 5). Scott discloses various screening rules that accept client input variables.

Regarding claim 17, Scott discloses:

wherein a screening rule further comprises one or more screened characters that, when detected in client input, are screened from the client input according to a screening rule (Scott, fig. 5 – see transformation).

Regarding claim 18, Scott discloses:

wherein the screening rule further comprises a default screening action that is applied in the absence of a specified screening action (Scott, fig. 5 – see transformation). Scott discloses a single screening action that is to be performed, and thus, a default screening action.

Regarding claim 19, Scott discloses:

wherein the screening rule further comprises a specified screening action that is applied to the screened client input (Scott, fig. 5 – see transformation). Scott discloses a single specific screening action that is to be performed.

Regarding claim 20, it is rejected, at least, for the same reasons as claim 5.

Regarding claim 21, it is rejected, at least, for the same reasons as claim 1, and furthermore because Scott discloses:

serving a web page to a client over a distributed network; receiving client input via the web page (Scott, fig. 1, page 2, col. 1, par. 3-6)*; comparing the client input with multiple and distinct client input security screens stored in a security declarative module; wherein the security declarative module includes a global section configured to screen all types of client input values and an individual values section configured to screen particular types of client input values* (see rejection of claim 1)*; if invalid client input is detected, performing a screening action on the invalid client input as indicated by the security declarative module* (Scott, page 3, col. 2, par. 2; page 4, col. 2, par. 3; page 6,

col. 1, par. 1, 2; fig. 5); *and wherein the client input security screens included in the security declarative module can be applied to multiple web pages* (Scott, page 4, col. 1, par. 2).

Furthermore, Scott discloses a computer system, and thus discloses media and instructions (Scott, fig. 1).

Regarding claims 24 and 25, they are the media and instruction claims corresponding to the method and system claims of 5 – 7, 18, and 19, and they are rejected for, at least, the same reasons.

Regarding claim *26*, Scott discloses:

wherein the screening action further comprises a default action that is not required to be specified in a client input security screen (Scott, page 6, col. 1, par. 1, 2).

Regarding claims *27* and 28, Scott discloses:

wherein the multiple web pages are included in a web project and *wherein the multiple web pages are included in a web-based application* (Scott, Abstract; Introduction; fig. 1; section 3.1; page 4, col. 1, par. 2; page 6, col. 1, par. 2, col. 2, par. 1). Scott discloses a security policy to be applied to a large web-application, the policy comprising rules for the web pages of a site. The web pages are associated with a web application, thus, they are included in a web project/application.

Response to Arguments

Furthermore, Applicant's arguments filed 9/22/2006 have been fully considered but they are not persuasive.

Applicants argue primarily that:

(i) As discussed during the interview, Scott does not first use a global section to screen input values and then use an individual values section to screen at least one of the client input values. In point of fact, Scott would appear to teach directly away from any such notion... Yet, Scott instructs in section 3.4 entitled "The Security Gateway" that the validation constraints are first employed (i.e. what the Office considers as the "individual value section") and then the transformations are employed (i.e. what the Office considers as the "global section"). (Remarks, pg. 11, 12)

In response, the examiner respectfully notes that the applicant misinterprets the reference of Scott and has provided evidence contrary to the applicant's assertions. In fact, the applicant has pointed out, with reference to section 3.4, that Scott teaches first an application of transformations (such as a global encoding transformation) and secondly an application of validation constraints (section 3.4, par. 3).

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

See Notice of References Cited.

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeffery Williams whose telephone number is (571) 272-7965. The examiner can normally be reached on 8:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

J. Williams
AU: 2137
JW

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER